

INFORMATION ASSURANCE TESTING:

JAMMING IS NO LONGER ENOUGH



Presented by Colonel Hugo Keyner
Commander, Electronic Proving Ground
Fort Huachuca, AZ
26 April 2001

REPORT DOCUMENTATION PAGE

Form Approved OMB No.
0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) 26-04-2001	2. REPORT TYPE	3. DATES COVERED (FROM - TO) xx-xx-2001 to xx-xx-2001		
4. TITLE AND SUBTITLE Information Assurance Testing: Jamming Is No Longer Enough Unclassified		5a. CONTRACT NUMBER		
		5b. GRANT NUMBER		
		5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Keyner, Hugo ;		5d. PROJECT NUMBER		
		5e. TASK NUMBER		
		5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME AND ADDRESS Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA22102		8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS Electronic Proving Ground Fort Huachuca, AZ		10. SPONSOR/MONITOR'S ACRONYM(S)		
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT APUBLIC RELEASE ,				
13. SUPPLEMENTARY NOTES				
14. ABSTRACT A briefing relating to IA testing.				
15. SUBJECT TERMS IATAC COLLECTION; Army C4I; IA testing				
16. SECURITY CLASSIFICATION OF: a. REPORT Unclassified		17. LIMITATION OF ABSTRACT Public Release	18. NUMBER OF PAGES 15	19. NAME OF RESPONSIBLE PERSON Fenster, Lynn lfenster@dtic.mil
b. ABSTRACT Unclassified		19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007		
c. THIS PAGE Unclassified				
Standard Form 298 (Rev. 8-98) Prescribed by ANSI Std Z39.18				

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503			
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED	
	4/26/2001	Briefing 4/26/2001	
4. TITLE AND SUBTITLE		5. FUNDING NUMBERS	
Information Assurance Testing: Jamming Is No Longer Enough			
6. AUTHOR(S)			
Keyner, Colonel Hugo			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)		8. PERFORMING ORGANIZATION REPORT NUMBER	
Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA 22102			
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
Electronic Proving Ground Fort Huachuca, AZ			
11. SUPPLEMENTARY NOTES			
12a. DISTRIBUTION / AVAILABILITY STATEMENT		12b. DISTRIBUTION CODE	
Approved for public release; Distribution unlimited		A	
13. ABSTRACT (Maximum 200 Words)			
A briefing relating to IA testing.			
14. SUBJECT TERMS		15. NUMBER OF PAGES	
IATAC Collection, Army C4I, IA testing		14	
		16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UNLIMITED

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102



Agenda

- ❖ EPG's role in Army C4I Testing
- ❖ Our approach to testing IA
- ❖ Challenges in IA Testing
- ❖ Thoughts on how to improve IA Testing

*An approach of IA testing for
Tactical C4I Systems*



EPG'S ROLE – Development Testing for Army C4I Systems

EXPERIMENTATION

AWEs

Division Capstone Exercise (DCX)
Joint Contingency Force (JCF)
Division XXI (DAWE)
Prairie Warrior
BDE TF XXI
Tactical Internet Demo
Warrior Focus
Focus Dispatch

Advanced Warfighting Experiments

ACQUISITION CYCLE

FBCB2

TEST EVENTS

FBCB2 IOTE
FBCB2 LUT3 (NTC)
FT3
FBCB2 LUT2/FDTE
FT2
FBCB2 LUT1
FT1
EPLRS
SINCgars
NTDR

ATCCS

TEST EVENTS

MCS TT
ISYCON TT
MCS IOTE
CSSCS IOTE
ASAS BLK II
MSE ATM

FIELDING FY00

FY 04

First Digitized Division

First Digitized Division

DIGITAL CORP

47 Years of Experience

**Leaders in Dynamic Test Control, Sim/Stim, Digital Data Capture,
with a Systems Approach to Test Design and Data Analysis.**



What is Information Assurance?

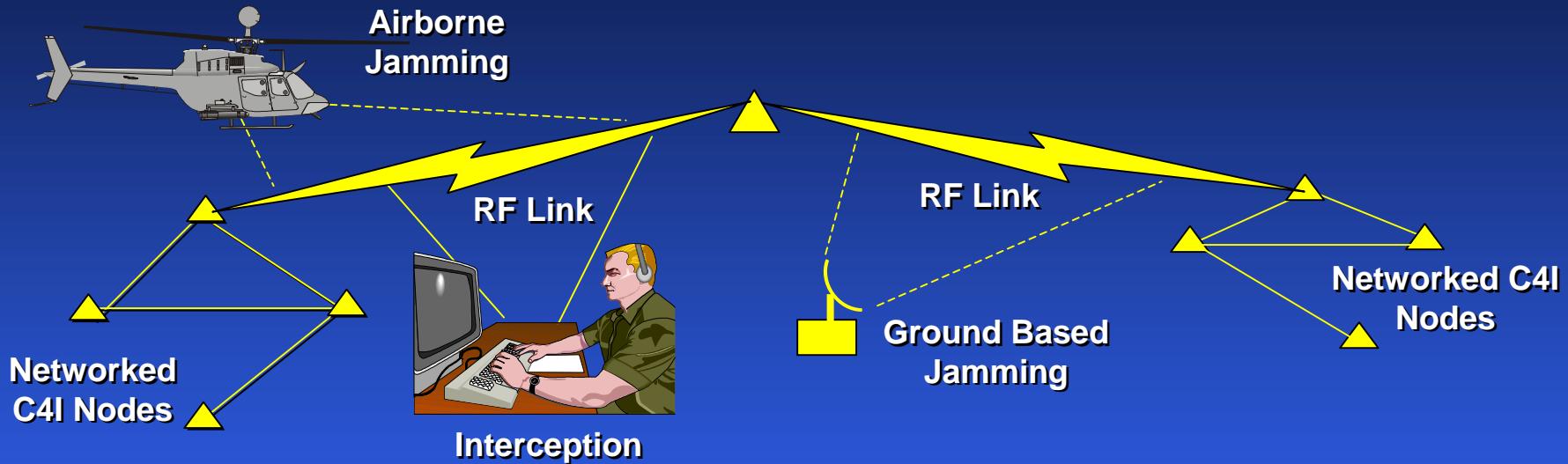
“Information Operations that protect and defend information and information systems by ensuring their availability, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.”

- Joint Pub 3-13

IA is not SECURITY (But Security is an important IA Subset)



The Old Paradigm – Focus on the RF Links



Things That Deny, Delay, Disrupt and Corrupt Information Flow

- *Jamming*
- *Co-Site*
- *Interception*
- *Xmtr/Rcvr Destruction*



What is the “Threat?”

◆ Sources

- NSA STAR
- DISA IASE
- FBI CyberNotes

◆ Threat Profile

- Natural Disaster
- Power Outages
- Poorly Configured Equipment
- Poorly Trained or Error Prone User
- Bad Trusted Insider (Biggest Single Threat)

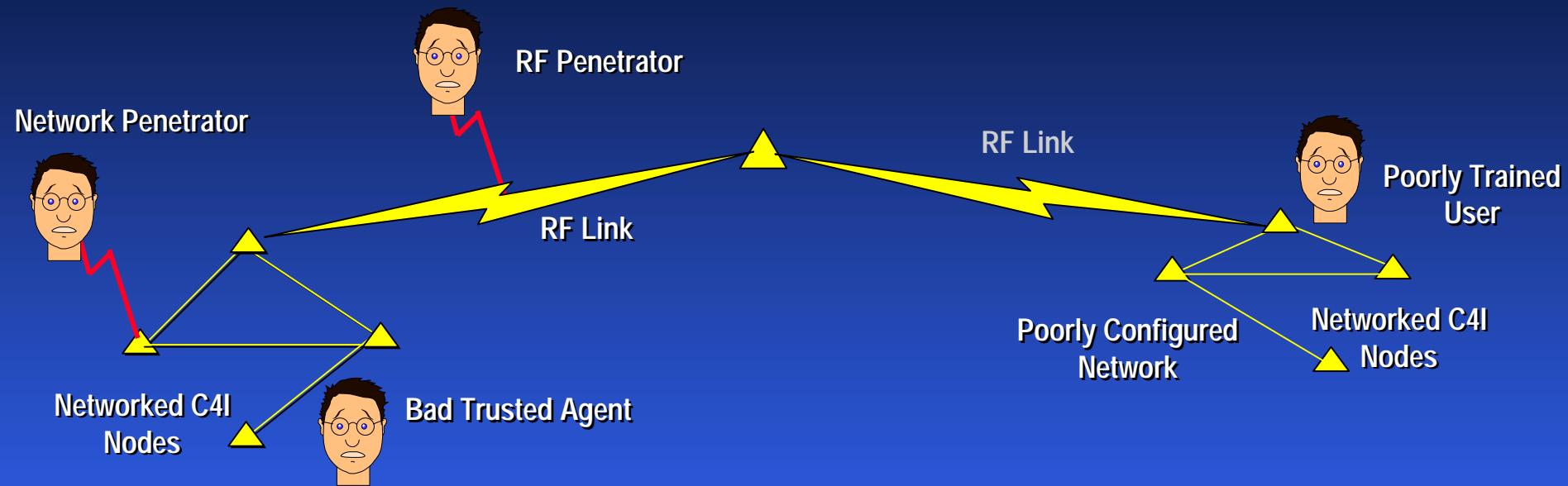
-----over 80% of threat-----

- External Hacker
- Malware (Trojan, Virus, etc.)

Aim is to deny, delay, disrupt, or corrupt information flow thereby denying us information dominance.



The New Paradigm – Focus on the Networks and RF Links

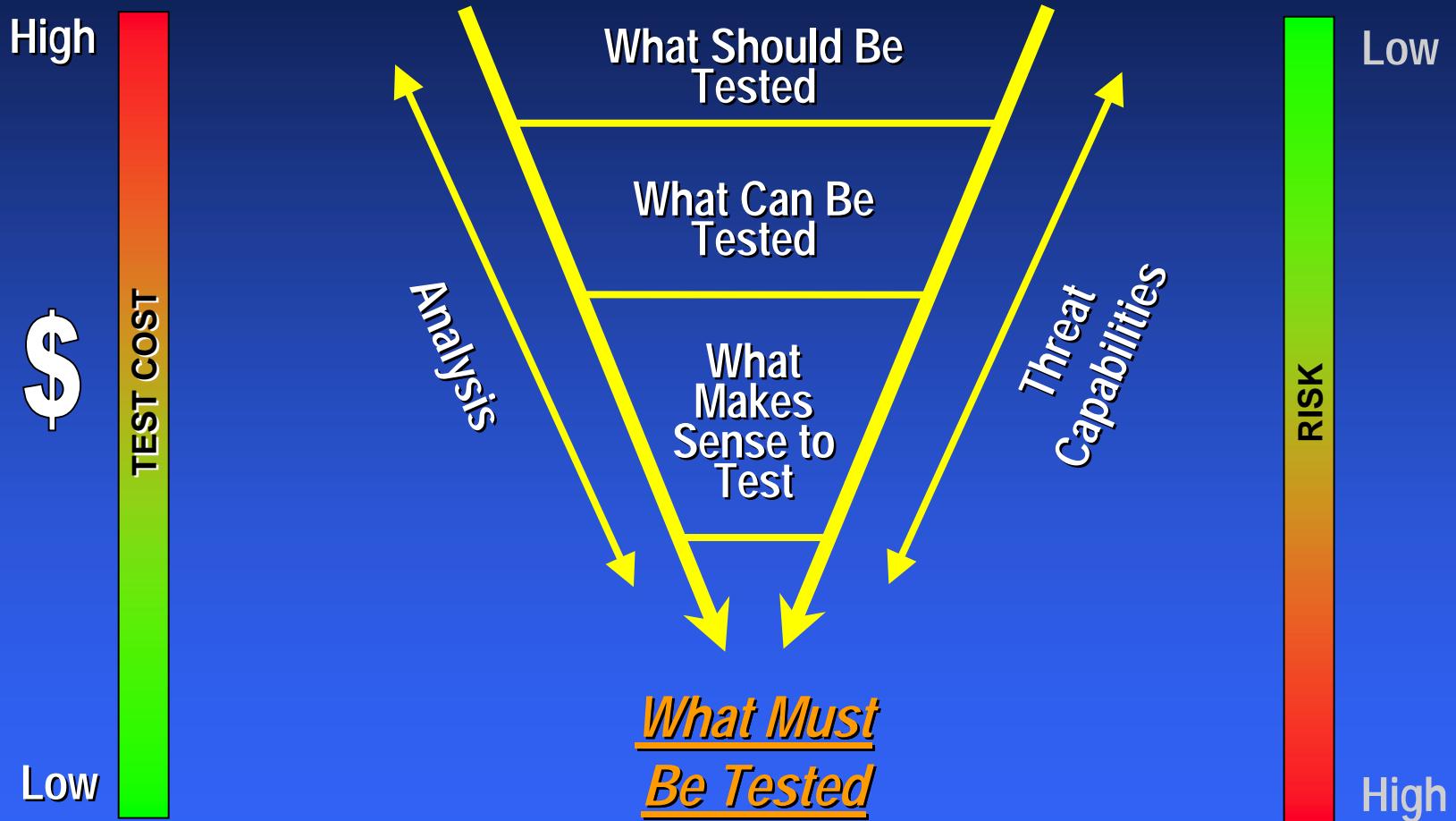


Things That Deny, Delay, Disrupt and Corrupt Information Flow

- **Poorly Trained User**
- **Viruses**
- **Bad Trusted Agent**
- **Xmtr/Rcvr/Node Destruction**

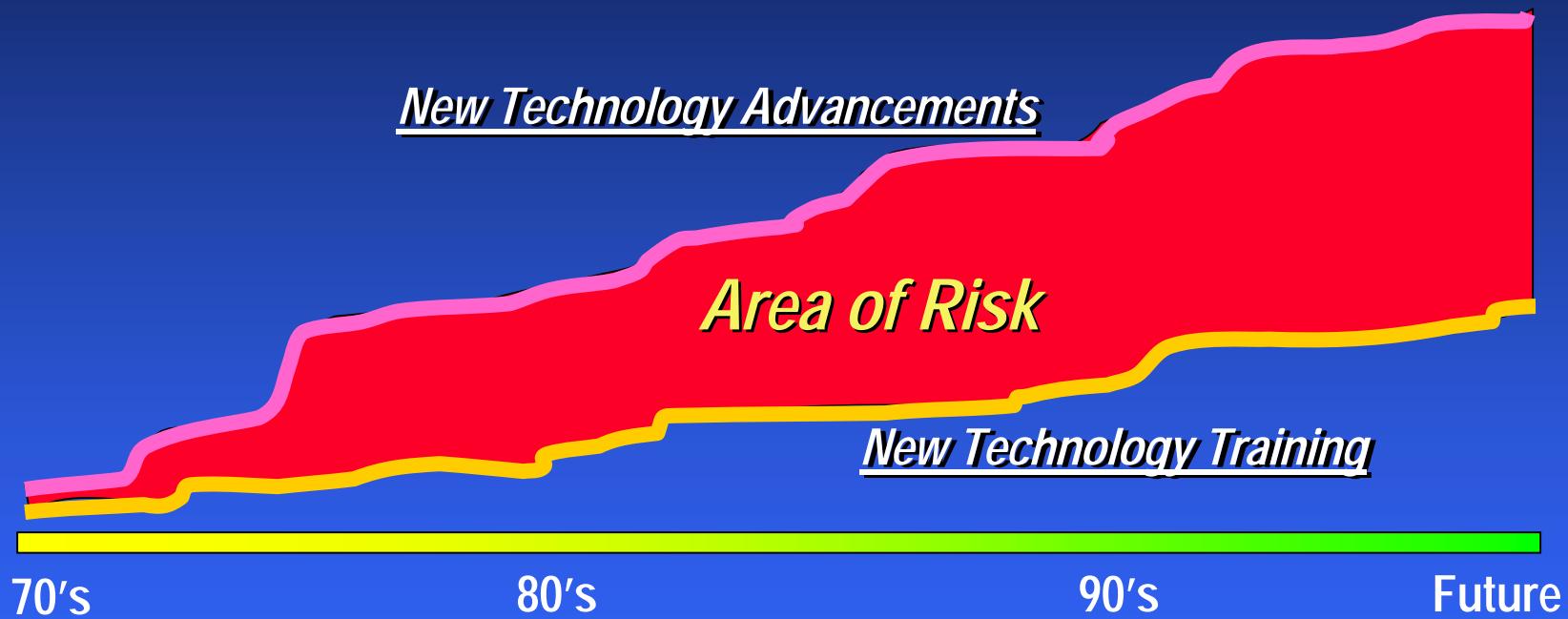


Developing a Strategy for IA Testing





Training Lag





Pragmatic Realities Related to IA Testing of a Tactical C4I System

- ❖ Should test technical and non-technical elements of IA. However, DiD Architecture, IA procedures, or IA related training may not be in place prior to DT.
- ❖ IA MOPs may have been addressed by another test venue (e.g., DITSCAP, JITC, etc.)
- ❖ If a DITSCAP is conducted – before or after DT?
- ❖ Programs are short of time and money. How can you afford not to do the “Must Be Tested”?

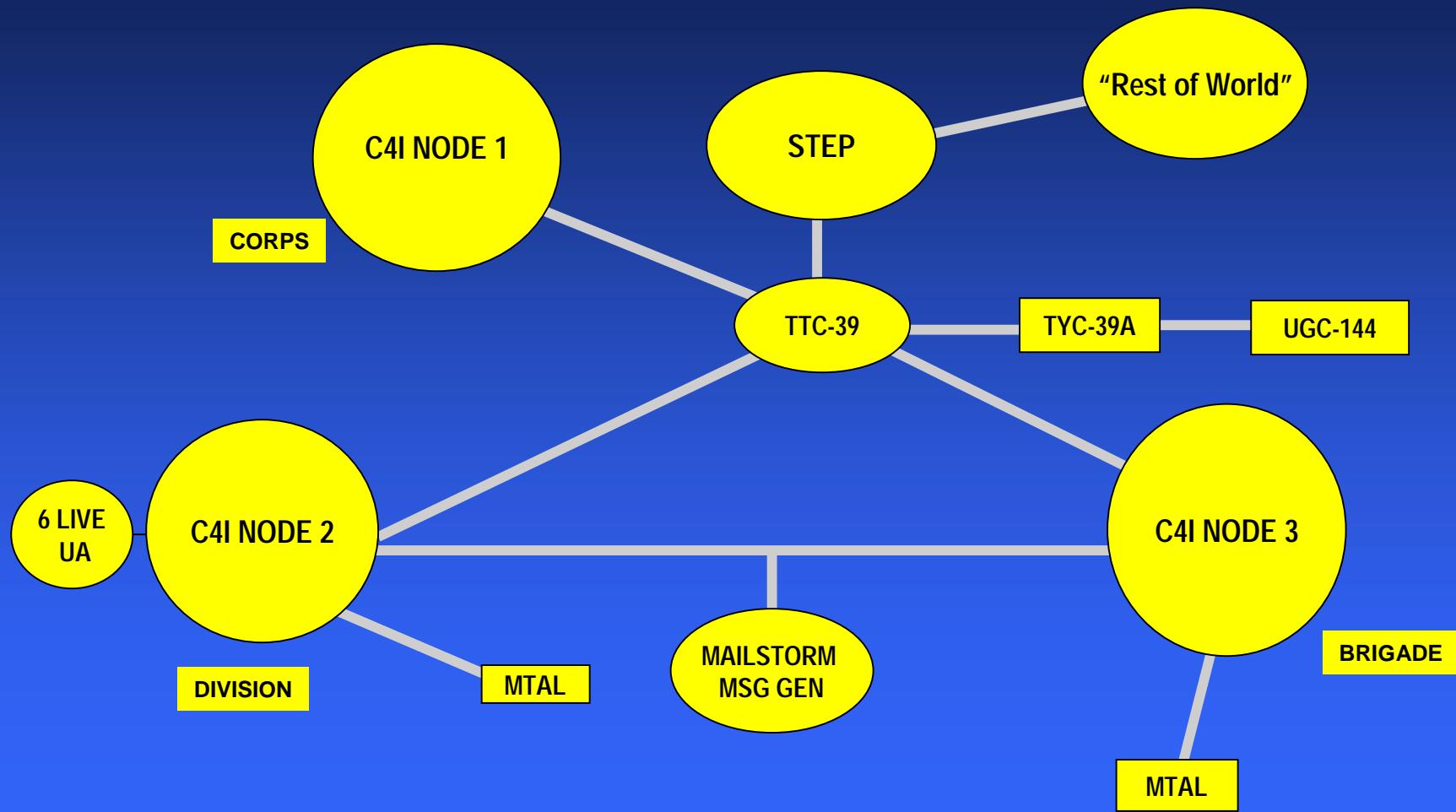


Key Elements in EPG's Approach to IA Testing of Tactical C4I Systems

- ❖ **Use C-TNOSC as “network monitor”**
- ❖ **Pursue parallel Red Team support from multiple sources (e.g., LIWA and 902nd)**
- ❖ **Added Special Requirements of Virus Testing**
 - **Conduct at end of Test Window**
 - **Insure physical isolation of Test Network**
 - **Protect Test Instrumentation**
 - **Conduct Post Test system sanitization**

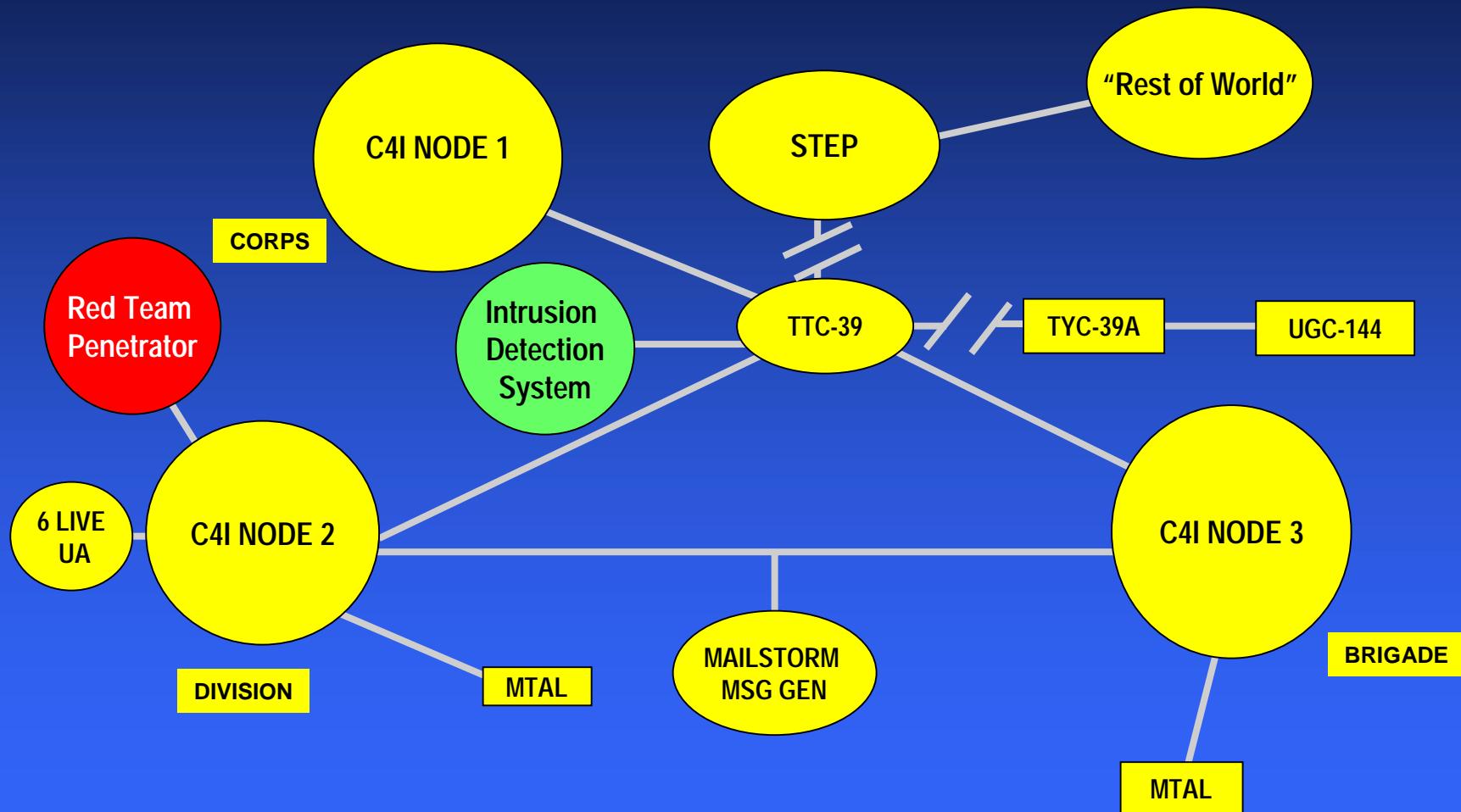


Typical Test Configuration - Performance Scenario





IA Test Configuration





Lessons Learned

- ❖ Use a “System of Systems” test approach.
- ❖ If a DITSCAP is done, then SSAA must be completed in time to support DT/OT planning.
- ❖ Cost effective IA Testing requires an integrated Test Strategy
 - Risk assessment, DITSCAP, DT and OT under the construct defined in DOT&E policy (include non-oversight programs).
- ❖ IA procedures and trained operators must be developed in a timely manner to support testing
 - DT and DITSCAP Phase II & Phase III offer the best opportunity for testing IA on Tactical C4I Systems.
- ❖ IA testing should be approached as a multi-organizational process.